County of San Bernardino
Department of Behavioral Health

Remote Access Policy

Effective Date 1/29/07
Approval Date 1/29/07

Allan Rawland, Director

Policy

It is the policy of the Department of Behavioral Health to standardize the physical attributes necessary to control the access to systems and data that may contain client ePHI and other departmental confidential data, to ensure its continued availability, confidentiality and integrity. The DBH Information Technology Unit is responsible for ensuring that the proper steps are taken to minimize, control and rectify any unauthorized access.

Purpose

To establish guidelines that define the functions to be performed, the manner in which such functions are to be performed, and the physical attributes for controlling remote access to the department's systems and data by business associates, vendors and workforce members.

Authorization

Remote access to the county's and/or department's systems may be authorized by Information Technology to allow vendors the capability to perform system software, application software and infrastructure maintenance, to provide contract agencies the ability to complete data entry or file uploads, and provide the department's business associates the capability to receive or deposit specific data identified in a "scope of work".

Remote Access

- All persons accessing the network, regardless of origin, must have a unique user-id and password that has been authorized and configured by Information Technology specifically for that purpose

- All persons accessing data that may contain client ePHI must have completed the county's/department's HIPAA Privacy/Security and application training requirements. **Vendors whose systems are in use by the department are excluded from this requirement**

- All remote connections must be:
  - ➢ Approved and controlled by Information Technology and be assigned a unique user-id and password.
  - ➢ Authorized, authenticated and secured before access to the network/system is granted.

- Remote access methods are:

- ➢ Virtual Private Network (VPN)
- ➢ Telnet
- ➢ DEC NET

Intrusion Detection Software

<u>County Network:</u>

- The county network is protected by a "Firewall" that prohibits users and or transmissions from gaining access to the various systems and data maintained by the Network Services Unit within the Information Services Department (ISD)

- The Data Security Unit (DSU) within ISD maintains a series of intrusion detection software applications that are monitored on a twenty-four hour basis to identify and report any unauthorized or suspicious access attempt

- The Data Security Unit will immediately contact the owner of an impacted system should an unauthorized or suspicious attempt to gain entry be detected

- DBH's Information Technology, working in collaboration with the DSU, will take the appropriate action to mitigate and resolve further unauthorized activity of this type

<u>County E-mail System:</u>

- The LAN Administrative Service Unit within ISD is charged with maintaining the email server data and preventing unauthorized or suspicious access by:

    - ➢ Installing, monitoring and maintaining intrusion detection software

    - ➢ Encrypting all data that resides on the E-mail servers

    - ➢ Quarantining suspected files that may contain unauthorized data and or viruses

    - ➢ Escalating security and or virus related issues to the DSU and potential departments that may be affected

- DBH's Information Technology, working in collaboration with ISD will take the appropriate action to mitigate and resolve all virus contamination that has impacted the department's LAN network

<u>Application Systems:</u>

- The Technical Operations unit (TSO) within ISD is charged with installing, monitoring and maintaining the intrusion detection software that monitors and reports any unauthorized access attempts impacting the DEC/VMS and SQL server environment on a twenty-four hour basis

- Software logs are reviewed on a daily basis and suspected concerns are escalated to the TSO management team and DBH's Information Technology Unit

- DBH's Information Technology, working in collaboration with TSO will take appropriate action to mitigate and resolve further unauthorized activity of this type
  - ISD's Network Services and Data Security Units will be notified if resolution of the unauthorized activity needs to be escalated for resolution

Violations

A staff that violates the use of DBH systems as described above or in other County policies will be subject to disciplinary action that can include termination of employment.